U.S. Department of State
Privacy Impact Assessment Summary

TITLE: Consular Shared Tables (CST)
May 2007

I. Describe the information to be collected (e.g., nature and source). Be sure to include any information in an identifiable form, e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc).

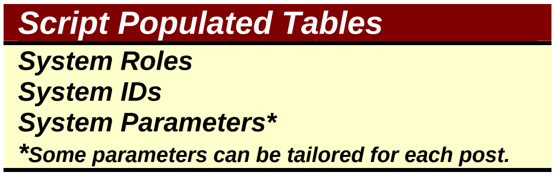
CST is a client-server based application. It resides on the Consular Affairs segment of the OpenNet and is deployed to all posts supporting consular operations. CST is one of CA's Major Application; and CST is responsible for storing and maintaining data reference tables and user information for all modernized systems. These tables will be used by several Consular Affairs applications to make functional, business decisions.

No personal information is stored by CST. CST's data consist of codes, lookup/control tables used in the processing of visas, passports, consular receipts, etc. An example of data is:

> Country Code Table that lists information such as country code, description, region, etc.

II. Why is the information being collected (e.g., to determine eligibility)?

System administration data, such as the following:



Script Populated Tables
System Roles
System IDs
System Parameters*
****Some parameters can be tailored for each post.***

Based on these tables, CST covers CST Administrators, Local System Administrators, Database Administrator(s), and regular functional users. The functional users consist of Washington-based users and Post-based users.

They will be responsible for updating reference tables as follows:

> Washington-based users: These users are responsible to update table data having relevance to all posts, worldwide.

> Post-based users: These users are responsible for updating the data relevant to their local post processing requirements.

No personal information is stored by CST. CST's data consist of codes, lookup/control tables used in the processing of visas, passports, consular receipts, etc. An example of data is:

> Country Code Table that lists information such as country code, description, region, etc.

III. How will the information be used (e.g., to verify existing data)?

To valid codes and authenticate Consular Section users at post.

IV. Will you share the information with others (e.g., another agency for a programmatic purpose)? If yes, list the entities.

No, CST will not share the information with others (e.g., another agency for a programmatic purpose).

V. Describe what opportunities individuals have been given to decline to provide information or to consent to particular use of the information (e.g., whether individual may withhold permission for a particular use).

This is not applicable to CST**;** no Visa applicant information is stored by CST. CST's data consist of codes, lookup/control tables used in the processing of visas, passports, consular receipts, etc.

VI. How will the information be secured (e.g., administrative and technological controls)?

The Bureau of Diplomatic Security is responsible for the investigations of personnel in conjunction with normal hiring practices. This investigation will consist of a review of a completed security questionnaire, a name check against applicable government, police, credit and fingerprint records, and may include a personal interview if warranted.

Once the highest-level background investigation available has been completed, cleared technical personnel (government and contractors) will be allowed to access, become a part of the development team and/or access the computer rooms housing CST; and no one is allowed to access the system until a limited background investigation has been completed. In addition, all domestic CA positions are reviewed for sensitivity level.

All Domestic and Overseas users must complete a Password Receipt Controls Form, acknowledge the Access Privileges Review procedures, sign the Rules of Behavior issued before access is given to the OpenNet. The users must also sign nondisclosure agreements, acceptable use agreements and conflictof-interest agreements that are also discussed and explained to the users before access is given to any CA/CST system to include CST.

All CST – CCD (Post and domestic) users must request a CCD account online through the CCD portal. They are to complete the form, acknowledge the Confidential Nature of Visa Record Acknowledgement Statement which includes the employee acknowledgement statement "I, John/Jane Doe, have read this "Briefing Acknowledgement Statement" on this date mm/dd/yyyy. I understand the handling and protection requirements for visa records. By signing this statement, I agree to abide by all legal and other requirements pertaining to these records" and electronically submit it to the CCD certifying authority in the Office of Children's Issues (CA/OCS/CI). The CA/OCS/CI approves and/or denies the request, however if the request is approved the user is notified.

Access to CST is limited to only authorize users. To ensure these users are valid, identification and authentication procedures are used. All users must first identify and authenticate to their CA domains via the CST workstation to gain access to OpenNet. Users must then identify and authenticate through CST when accessing the CA applications. Each user is provided a unique identifier (userid) by a CST System Administrator. This userid is created according to 12 FAM policies, is maintained by the CST system administrator, and complies with the following DoS userid format:

{Last name}{First initial}{Middle initial (if applicable)}

Incorporating the user's name into the userid allows for correlation between the user's activity on the system and his or her identity. The CST Administrator defines the CST user's role. This is accomplished within the CST (Consular Shared Tables) application. Once defined within the CST application, all other CA application administrator that utilizes CST defines their user's roles within the CA applications that utilize CST. When it is determined that a user no longer needs access, the user account will be disabled.

Within the certified and accredited (C&A) boundary of CST, only cleared technical personnel shall be allowed to access the components and no one shall be allowed to access the system until the appropriate background screening has been completed. This screening is conducted prior to the individual employment to provide a basis for ensuring his/her employment is clearly consistent with the interests of the National Security and all information system positions shall be designated in terms of sensitivity. Due to *privileged user* status the following administrators must restrict themselves from using their position to turn off/destroy audit trails, not to give unauthorized individuals privileged access, and modify the system to negate automated security mechanisms: System and Database Administrators.

CST supports three user groups:

- System Administrators/Users Security
- Database Administrators
- CST end-users

All CST users receive their access through local access requesting procedures organic to the CA organization and compliant with 12 FAM. Each user must submit an account request form indicating the requirement for system and database administrator or CST end-user privileges. The account request is reviewed by the user's supervisor and must be approved by the manager before the request can be granted.

CST end-user access is determined based on their approved user role.

The ISSO, the system manager, and the end-user's supervisor structure access privileges to reflect the separation of key duties that end-user perform within the functions the application supports. Access privileges are consistent with the need-to-know, separation of duties, and supervisory requirements established for manual processes.

Once they are properly identified and authenticated by the system, the internal DoS user is authorized to perform all functions commensurate with the job requirements. In an effort to restrict users to only these required functions, logical access controls are utilized in accordance with the principle of least privilege and the concept of separation of duties. The specific CST users' role must be identified by the user's manager requesting access for the identified user. CST privileges relate directly to rights assigned to groups and user accounts associated with the directory services. A "right" authorizes a user to perform certain actions on the system and any user who logs on to an account to which the appropriate rights have been granted can carry out the corresponding actions. When a user does not have appropriate rights, the system blocks attempts to carry out those actions.

Once the user account has been created, the appropriate privileges are assigned to the user based on the requirements of their job functions, but limited to only the required privileges. This includes restricting the user's access to data files, peripherals, and their processing capability.

The CST System Security Plan (SSP) documents the criteria, procedures, controls, and responsibilities regarding access.

The CST system is protected by NIST SP 800-53 mandated Moderate Technical, Management and Operational security controls which include access, audit, configuration management, personnel controls for all users to the system, computer rooms, media; and all CA operating systems must comply to DS security configuration for Windows 2000 /2003, Oracle, ASP.NET 1.1, etc.

VII. How will the data be retrieved (e.g., will it be retrieved by a personal identifier such as name, social security number, address, telephone number or some other identifier that is unique to an individual)?

This is not applicable to CST. No personal information is stored by CST. CST's data consist of codes, lookup/control tables used in the processing of visas, passports, consular receipts, etc. An example of data is:

> Country Code Table that lists information such as country code, description, region, etc.